

## Firewall-1 and ISA D.o.S.

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2002-02/0265.html>

---

**From:** [overclocking a la abuela@hotmail.com](mailto:overclocking_a_la_abuela@hotmail.com)

**Date:** 02/17/02

Date: 17 Feb 2002 15:18:13 -0000

From: <[overclocking\\_a\\_la\\_abuela@hotmail.com](mailto:overclocking_a_la_abuela@hotmail.com)>

To: [vuln-dev@securityfocus.com](mailto:vuln-dev@securityfocus.com)

('binary' encoding is not supported, stored as-is)

Hi,

last year I reported a denial of service to Firewall-1 : flooding on port 264 ( fw1\_topo ). Check Point was not able to reproduce this attack so they never recognise it as a real problem. Now, many security concerned sites have this behaviour in their firewalls bug lists.

You can stop this attack if you manually create all the rules and limit the acces to this port ( 264 ) only to clients that need it. But there was a special situation : a firewall that accepts connections to fw1\_topo with ANY as source to allow Securemote connections with a dinamic IP address...

For this D.o.S. to success you needed a fast link so the only real scenario was to attack from the internal network.

Probably, too many requisites needed,...OK.

So, what If I am an external attacker ?

I can build a trojan and mail it to some internal user of the target network. The trojan will send packets to some external IP, to force them to pass trough the Firewall-1. This time, we do not need to know the Firewall IP , we only send a lot of packets to port 80 with the SYN flag. Simply, rude but effective. My tests always finish with the firewall completely frozen.

The firewall machine is a Professional Win2000, PII 350 with 320 MB. Link is a 10 MB ethernet.

The software used is ippacket. Now the packet we build is :

## SecurityFocus Vuln-Dev: Firewall-1 and ISA D.o.S.

-source : valid internal IP ( does not matter )  
-dest : external IP  
-source port : 10000 ( does not matter )  
-dest port : 80 ( probably the firewall rules accept it )  
-flags : SYN  
-mode : -1 ( continuous mode )

In the case of Microsoft ISA Server I have been trying some types of packets to flood it, and the one it seems to freeze the firewall is this ( land ):

-source : internal ISA IP  
-dest : internal ISA IP  
-source port : 8080  
-dest port : 8080  
-flags : SYN  
-mode : -1 ( continuous mode )

And the ISA stops responding : clients will not be able to surf the web, ISA machine does not respond ( CTRL + ALT + SUP does not work ), ... This tests has been done with an ISA configured with http proxy on port 8080 on a Win2000 Server.

Generally, I think is not difficult to smash a firewall if you are on the local network. You only have to find wich packets will force the forwarding/filtering device to work hard : if the firewall uses proxies, some kind of authentication, some statefull inspection, etc, then it is an easy job. Now, it seems that old packet filters are more efective on defending this attacks, since they do not do a deep inspect...

So, is this a general flaw on modern firewalls ?  
Are they unable to manage large ammount of connections requests ?  
Bad guys are not only in the wild, they can be in your network, or they can begin an attack from your internal network with a trojan.  
Please I would agree some feedback.

Hugo Vázquez Caramés  
Security Consultant  
Barcelona  
SPAIN

---

• *Previous message:* [Larry W. Cashdollar: "Re: slocate bug."](#)

SecurityFocus Vuln-Dev: Firewall-1 and ISA D.o.S.

- *Next in thread:* Dom De Vitto: "RE: Firewall-1 and ISA D.o.S."
- *Reply:* Dom De Vitto: "RE: Firewall-1 and ISA D.o.S."
- *Reply:* Lincoln Yeoh: "Re: Firewall-1 and ISA D.o.S."
- *Reply:* overclocking a la abuela@hotmail.com: "Re: Firewall-1 and ISA D.o.S."
- *Reply:* overclocking a la abuela@hotmail.com: "Re: Firewall-1 and ISA D.o.S."
- *Reply:* Jim Harrison (SPG): "RE: Firewall-1 and ISA D.o.S."
- *Messages sorted by:* [ date ] [ thread ] [ subject ] [ author ] [ attachment ]